Economist Intelligence Unit

The Economist

Complying with rules for identity management

An Economist Intelligence Unit briefing paper sponsored by IdenTrust

Preface

Complying with Rules for Identity Management is an Economist Intelligence Unit briefing paper, sponsored by IdenTrust. The Economist Intelligence Unit bears sole responsibility for this report. The Economist Intelligence Unit's editorial team executed the survey, conducted the interviews and wrote the report. The findings and views expressed in this report do not necessarily reflect the views of the sponsor. Russ Banham was the author of the report and Rama Ramaswami was the editor. Richard Zoehrer was responsible for layout and design.

Our research drew on two main initiatives. We conducted a global online survey in May and June 2006 of 127 executives from various industries. To supplement the results, we conducted in-depth interviews with executives from around the world familiar with identity management regulations and authentication technologies. Our thanks are due to all survey respondents and interviewees for their time and insights.

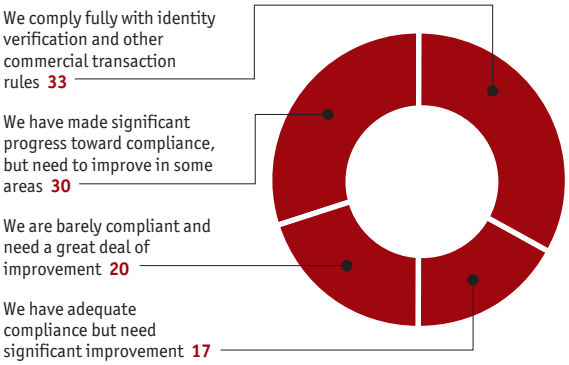
December 2006

Executive summary

As more companies use the Internet for electronic transactions, the risk of network infiltration and information theft has soared. This has prompted governments to institute regulations designed to curb the growth of online fraud, identity theft and money laundering. Well-publicised cyber crimes involving the appropriation and misuse of personal and corporate identities and the theft of privileged data have damaged consumer trust in e-commerce and threatened corporate security. Not surprisingly, governments are putting the onus on companies to authenticate the identities of their counterparties. Consumers are also demanding that their identities be protected.

In recent years, several governments worldwide have instituted electronic commerce laws that directly or indirectly require companies to reduce their vulnerability to identity theft. The United States, the European Union, Korea, Brazil, Japan, Australia, Singapore and many other nations have drafted or implemented regulations to safeguard consumer privacy, protect corporate data integrity and enhance auditing accountability. Standards to combat money laundering and terrorist financing that include customer identification have been proposed by the Financial Action Task Force (FATF), an inter-governmental organisation, and have been adopted by more than 150 jurisdictions. In large part, these rules call for companies to adopt stronger identity authentication measures to assure governmental authorities about the veracity of their electronic transactions. Current and prospective regulations have created a boom in the interest in and use of identity authentication technologies such as digital certificates, biometrics, one-time passwords (OTP) and tokens.

A. Which of the following statements best describes your organisation's level of compliance with regulations governing the global supply chain such as account authentication rules?
(% respondents)



Source: Economist Intelligence Unit

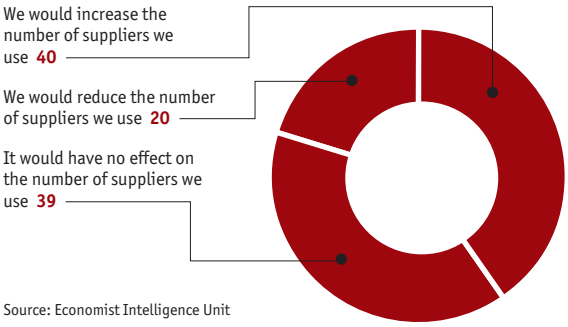
In preparing this briefing paper, the Economist Intelligence Unit conducted a survey of 127 senior executives from both large organisations and small and midsize enterprises (SMEs). Among the main conclusions drawn from this survey are:

- Nearly 40% of survey respondents fear a security breach of their computer systems, while 32%

About our survey

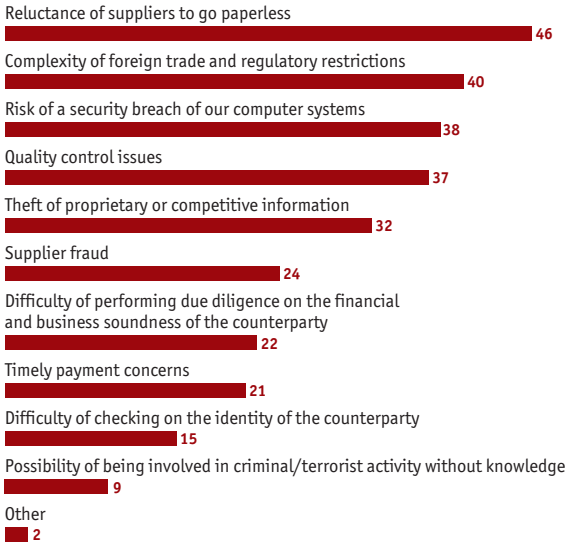
In May and June 2006 the Economist Intelligence Unit queried 127 executives on their global supply chain operations and identity management practices. Approximately 31% replied from western and eastern Europe, 40% from the Americas and 29% from the Asia-Pacific region and other parts of the world. Respondents represented a wide range of industries and functions; 28% cited manufacturing as their primary industry. About 50% of the respondents were C-level executives or board members. At 72% of the total sample, companies with less than US$500m in annual revenue were the most heavily represented group.

B. What effect would it have on your procurement practices, if your company were able to authenticate the financial stability of suppliers?
(% respondents)



Source: Economist Intelligence Unit

C. What do you consider to be the greatest risks of automating your company's global supply chain?
Select 3 options (% respondents)



Source: Economist Intelligence Unit

are concerned about the theft of proprietary or competitive information (see chart C).

- More than a fifth of survey respondents (20.31%) say they are "barely compliant" with regulations governing account authentication and "need a great deal of improvement" (see chart A, pg. 4).
- More than 40% of respondents say they would increase the number of suppliers they use if they were able to authenticate their financial stability (see chart B).

The survey indicates that many companies are just as concerned about the risks of the Internet as they are captivated by its global networking capabilities. While compliance with government regulations on electronic commerce, identity theft, money laundering, privacy and data integrity requires time, expense and effort, such rules are necessary to preserve the extraordinary benefits presented by online cross-border transactions.

Identity theft on the rise

Government regulation of identity authentication has increased following the extensive losses that businesses have suffered because of identity fraud. Globally, losses from identity theft soared from $221 billion in 2003 to $2 trillion in 2005, estimates the Boston-based research firm Aberdeen Group. Nearly nine million people in the US have been victims of identity fraud in 2006, according to the 2006 Identity Fraud Survey Report, released by the US Council of Better Business Bureaus and Javelin Strategy & Research. The total one-year cost of identity fraud is estimated at $56.6 billion.

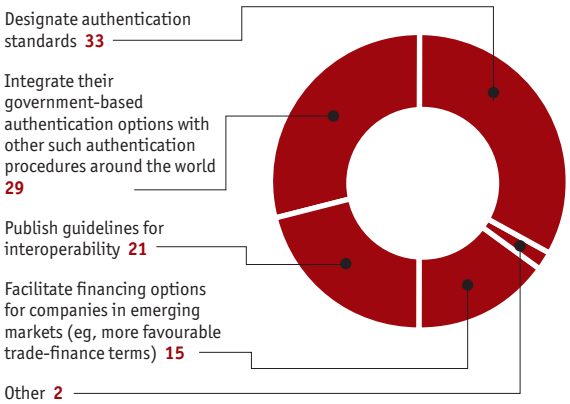
"All enterprises, not just financial institutions, must reconsider their identity authentication practices."

Principal, Acuity Market Intelligence

Throughout the World Wide Web, the threat of fraud is dire. In a 2005 survey of 5,000 Web banking users, conducted by technology research firm Gartner, one in three reported buying fewer items online than they would otherwise because of security concerns. Internet attacks have forced three-fourths of the respondents to log in less frequently and 14% to curtail online banking activities. Major concerns cited in the report are the rising instances of unauthorised access to personal information and lost consumer data files.

In the global corporate arena, companies are deeply concerned about identity authentication. About 67% of respondents to the EIU survey state that they need to improve their organisation's level of compliance with regulations such as account authentication rules that govern the global supply chain. Respondents identify designating authentication standards (33%) and integrating worldwide authentication options (29%) as the top two steps necessary to safeguard the global supply chain and ensure the safety of online commerce (see chart D). Without the use of identity authentication technology, companies must merely assume veracity—a highly risky undertaking.

D. What is the single most important step that individual governments and the UN could do to safeguard the global supply chain and ensure that more companies are integrated into it?
(% respondents)



Source: Economist Intelligence Unit

Although financial institutions are most vulnerable to identity scams, companies of all types are increasingly at risk. "All enterprises, not just financial institutions, must reconsider their identity authentication practices," says Maxine Most, a principal at Acuity Market Intelligence, a Boulder, CO-based strategic marketing consultancy. "In a way, Internet crime has replaced petty crime. You can get information about individuals and organisations and use that to steal money. Why pull a gun at a convenience store when you can sit comfortably at home with a computer and steal?"

Identity managment regulations: A global round-up

Countries around the world have issued a dizzying list of regulations that institutions must comply with to protect privacy, foil hackers, secure online commerce and communication and provide reporting. Nearly all of these laws mandate identity authentication to some extent. The following is a summary of current and proposed regulations and identity authentication trends in various countries and regions worldwide.

International: Anti-money laundering laws

One of the key watchdogs in this area is the Financial Action Task Force (FATF), an inter-governmental organisation created in 1989 to issue policies to combat money laundering and, beginning in 2001, terrorist financing. The FATF has 33 members, and its standards have been endorsed by more than 150 jurisdictions around the world. One of its main recommendations is for financial institutions and designated non-financial businesses to implement due diligence (CDD) procedures, including verifying the identity of customers when establishing business relations and carrying out certain transactions. CDD procedures also need to be followed when there is suspicion of money laundering or terrorist financing, or if doubts arise about previously obtained customer identification data. Organisations must conduct identity authentication by using reliable, independent documents, data or information. Non-compliance with the FATF's Forty Recommendations, a complete set of measures against money laundering, can result in financial institutions giving "special attention" to transactions with countries that do not comply, and possibly to the loss of those countries' membership in the FATF.

US: Greater data security. The Gramm-Leach-Bliley Act, passed in 1999, requires US financial institutions to ensure the security and confidentiality of their customers' non-public information. This legislation "fomented a rush for authentication technologies that ensured appropriate access to data and protected customer information travelling over a public network," says Jonathan Penn, an analyst at the consulting firm Forrester Research in Boston.

Gramm-Leach-Bliley was only the beginning. In 2001, the Federal Financial Institutions Examinations Council (FFIEC), an interagency body that prescribes uniform principles and standards for the federal examination of US financial institutions, offered guidance ("Authentication in the Internet Banking Environment") for creating and maintaining information security programs. Following concern about rising cases of identity theft, as reported in a December 2004 study by the Federal Deposit Insurance Corporation (FDIC), the FFIEC revised its guidance in 2005. Jeff Kopchik, senior policy analyst at the FDIC, notes that the new guidance "fleshed out the paragraph on authentication that was in the 2001 FFIEC guidance." The FFIEC has given banks until the end of 2006 to improve their online security systems, urging them to go beyond conventional user IDs and passwords to use what is known as multifactor authentication, or the combination of something the user is (such as a fingerprint or signature), has (such as a security token or software token) and knows (such as a password).

Among the authentication methods that banks can choose are hardware tokens, biometric identifiers like fingerprint and iris scans, passwords that can be used only once, or emerging risk-based multifactor authentication tools that include digital

certificates and a public key infrastructure (PKI). The latter, based on public key cryptography, involves the use of an encrypted key pair created through an algorithm. This is a combination of a company or individual's public key, which everyone can see on the Internet, with a private key, which only the recipient has.[1]

Several other pieces of legislation in the US compel the use of stricter identity authentication protocols. A "Know your customer" obligation was created in Section 326 of the US Patriot Act of 2001. The legislation requires financial institutions to verify each new account holder's identity before opening the account. "One of the largest vulnerabilities of financial institutions comes when opening a new account, since we don't have a track record with the customer or any information with respect to anomalies," explains Doug Johnson, senior policy analyst at the American Bankers Association.

Organisations also need to report enough information about the flow of transactions to identify where material misstatements due to error or fraud could occur.

The Sarbanes-Oxley Act of 2002 (SarBox) more indirectly invites enhanced identity authentication. The act was passed in response to major corporate and accounting scandals and enhances companies' record-keeping and disclosure requirements. It mandates companies to track information about how significant transactions are initiated, authorised, supported, processed and reported. Companies should be able to confirm that only authorised users have access to sensitive information and systems, and must enforce password security policies. Organisations also need to report enough information about the flow of transactions to identify where material misstatements due to error or fraud could occur.

"SarBox is designed for corporate integrity purposes, to ensure that financial statements and recorded income and expenses are indeed what they purport to be," says Jim Wills, anti-money laundering business line manager at Fortent, a New York-based provider of risk management solutions. "From a corporate perspective, this may imply a need to validate for compliance purposes that a supplier, for instance, indeed did give me the product I paid for and the monies went where they were supposed to go. This, of course, requires identity authentication."

Thomas Yee, CEO of Singapore-based GridNode, a business-to-business specialty communications software provider, points out that many SarBox requirements cannot take place without identity authentication: "SarBox spells out what companies can and cannot do when it comes to financial reporting, confidentiality and document integrity, although it does not provide executive guidance on how to implement proper processes. Authentication processes and digital certificates can make these compliance requirements happen."

European Union: Authenticating cross-border transactions. The US is not alone in its quest to improve Internet security and identity authentication. In 1999, the European Union issued the directive "Community Framework for Electronic Signatures." The directive aimed to facilitate the use of digital signatures and contribute to their legal

[1] Digital certificates depend on a PKI to assure secure transactions. A digital certificate is an electronic "credit card" that establishes an individual's or company's credentials when conducting online business. Issued by a certification authority (CA), the certificate contains the user's name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the issuing authority so that a recipient can verify that the certificate is real. Digital certificates can be kept in registries so that authenticating users can look up other users' public keys.

recognition, while establishing a legal framework for the services provided by digital certification organisations. The directive states that "rapid technological development and the global character of the Internet necessitate an approach which is open to various technologies and services capable of authenticating data electronically."

In 2005, the EU issued a Money Laundering Directive that outlines cases that require customer due diligence and describes the information that financial institutions must obtain. To protect citizens, the Data Protection Directive, which applies to transactions over the Internet, was issued in 1995. This directive states that the personal data of all citizens has equivalent protection in all member states.

The European Commission's plan to establish a Single European Payments Area (SEPA) by 2008 would replace separate domestic payment schemes. SEPA would oblige banks to charge the same fees and provide the same levels of service for cross-border euro retail payments as they presently do domestically. Another important EU regulation, the Markets in Financial Instruments Directive, or MiFID, is based on the introduction of a single market and regulatory regime for investment services across the EU. Every cross-border transaction requires an audit trail and validation of all parties involved in the transaction. MiFID also contains "Know your customer" requirements that necessitate identity authentication. "Once you move into an electronic world, that requires trust," explains Steven Hartjes, a partner in the financial services department of global accounting firm Ernst & Young in Amsterdam. "And trust requires identity authentication."

Identity verification is also a component of electronic invoicing, recognised by EU authorities since July 1st 2003, following the issuance of EU Directive 2001/115. The directive seeks to harmonise, simplify and modernise invoicing obligations on traders when they sell goods or services that are subject to value added tax (VAT). The legislation creates an EU legal framework for electronic transmission and storage of invoices,

SWIFT slammed for breaking data protection laws

Although it is rapidly becoming possible to pinpoint the identity of individuals and monitor every detail of their online transactions, organisations can run up against legal hurdles if they do so. Such is the case with the Society for Worldwide Interbank Financial Telecommunication (SWIFT), which manages international payments of $6 trillion a day between 7,800 financial organisations. Since the terrorist attacks of Sept. 11th, 2001, SWIFT has allowed the US government to access details of its transactions. In March 2006, however, the Belgian Data Privacy Commission contended that SWIFT broke privacy rules in handing its clients' records over to the US Treasury. This was followed by the Federal Data Protection Commissioner of Switzerland, Hanspeter Thür, stating in October 2006 that Swiss banks broke data protection laws when they failed to inform customers that SWIFT was transferring their information.

The situation highlights the emerging conflict between national security and personal privacy. A statement from SWIFT said that the behaviour of its US office was legal, due to "valid and compulsory subpoenas." With regards to Europe, it said that "SWIFT also did its utmost to comply with the European data privacy principles of proportionality, purpose and oversight." However, the Belgian Data Privacy Commission reports that "it must be considered a serious error of judgement on the part of SWIFT to subject a massive quantity of personal data to surveillance in a secret and systematic manner for years without effective grounds for justification and without independent control in accordance with Belgian and European law."

A European Commission working party of data protection officials has expressed "concerns about the lack of transparency" of this arrangement. The working party will decide whether or not to launch an independent audit. Mr Thür has urged that a solution be negotiated according to which US laws and European data protection rules are standardised.

enabling advanced electronic signatures or electronic data interchange to be used to guarantee the authenticity of origin and integrity of the contents of an invoice.

Another EU identity management measure deserves note. In 2003, member states agreed to embed computer chips containing a person's biometric data, such as fingerprints and unique iris characteristics, in passports, as a way to reduce counterfeiting and fraud. Biometric chips also will be embedded in visas issued to foreign nationals travelling to Europe. The deadline for the mandatory biometrics on passports and visas is 2008.

Asia: Moving towards digital security. In the Asia-Pacific region, South Korea leads other nations in developing regulations governing Internet security and identity authentication. "South Korea is pretty advanced in the development of a public key infrastructure," says Andrew McLauchlan, founder of 443 Proprietary Ltd, a Sydney, Australia-based technology consultancy. "The rest of Asia lags, although there have been significant advancements in Singapore, Japan and Australia."

Jae Yol Kim, CEO of GT Trust Korea, a Seoul-based identity management consulting firm, says, "As e-trading volume increased rapidly, more online trade problems and fraud occurred. With this in mind, the government revised its early e-trade and digital signature laws and set up a government-controlled Certification Authority, the Korea Information and Security Agency, for the PKI-based digital signature system in the country."

In 2005 there were more than 12 million digital

Securing the product package

Identity authentication is critical to Nationwide Financial's goal of sending information securely over the Internet to its partners in the financial services industry. The Columbus, OH-based company, part of the Nationwide Mutual Insurance Company, bundles together a mix of investment products like variable annuities and mutual fund wraps from its own shelves and from joint venture partners and then "sells" the package to investment brokers. The key to making the process efficient, seamless and secure is the use of digital certificates as part of a multifactor authentication approach. Digital certificates provide the authentication required when Nationwide Financial's server transacts with its partners' servers.

When investment professionals log onto National Financial's Web site to create a portfolio of products for their clients, there is a "seamless transition" from the company's site to its partners' sites, says Tim Lyons, Nationwide Financial's vice president of sales technology. "Several sites are bundled together, without the need for the broker to log onto each site separately."

The same concept is at work today on many travel sites on the Internet, where a customer can schedule a flight, book a rental car and reserve a room at a hotel all on the same site, despite these arrangements being made behind the scenes with three separate parties. "Brokers aren't aware of what is going on in the background—they just log on and our security model passes their information to our partners' Web sites," explains Guru Vasudeva, enterprise chief architect at Nationwide Financial. "The technology makes investment professionals' jobs efficient and convenient. And it gives us a competitive advantage through our partnership model."

Mr Lyons concurs: "From an economic perspective, the technology enables corporations to create a logical view of products and services easily transcending their corporate boundaries. I can glue partners together and create new value propositions at very low cost in a virtual way. That is a compelling opportunity, but it requires the secure exchange of information between partners. "

certificate users (80% individual and the rest corporate) in South Korea, out of a population of 44 million. Although the digital certificates affect only domestic online transactions, the South Korean government is cooperating with IdenTrust, a US-based provider of digital certificates, to deliver global interoperability in digital authentication and identity management. When completed in 2008, the platform will represent the world's first fully integrated electronic trading platform.

Mr McLauchlan says other countries in Asia are learning from South Korea's example. "In Japan, which has not formally regulated online security as yet, there is a regulatory framework for the use of electronic commerce and digital certificates to bind contracts, and many banks are thinking about public key infrastructure as a means to secure banking services," he explains.

Singapore was one of the first countries in the world to enact a law addressing digital security issues. The country passed an Electronic Transactions Bill in 1998, based closely on the model e-commerce law of the United Nations Commission on International Trade Law. Singapore has developed a PKI and is in the process of appointing a Controller of Certificate Authorities to license sector-specific Certification Authorities. At present, online banking access requirements remain password and personal identification number (PIN). "There are initiatives within the banking industry and the government to push for multifactor authentication to enhance the security framework of Internet banking," says GridNode's Mr Yee.

In Australia, the government has adopted a gatekeeper approach as its regulatory apparatus for deploying PKI. "The Australian government's role is to establish a regulatory framework and then let the private sector invest in it," Mr McLauchlan explains. "Consequently, the government has chosen not to set up its own PKI." Tony Burke, director of security issues at the Australian Bankers Association, says that "several individual financial institutions have themselves, in a number of cases, introduced stronger identity authentication. We also have gotten together as an industry to develop a set of authentication guidelines that are risk-based, allowing individual financial institutions to make their own decisions on risk management techniques relevant to their customer base, products and technologies." He notes that the country is in the thick of drafting legislation to combat money laundering and terrorist financing. "Identity authentication will be an important component of these actions," Mr McLauchlan predicts.

Singapore was one of the first countries in the world to enact a law addressing digital security issues.

He adds that India has a regulatory framework in place, "but is struggling to incarnate it into reality." Both India and Singapore are members of the Asian Economic Group, which, says Mr McLauchlan, is "looking very closely at identity authentication for cross-border online trade."

Latin America: Developing e-commerce regulations. Several Latin American countries are creating regulations on electronic commerce and digital signatures. "The realisation among Latin American countries was that if they waited [to introduce regulations], their banks would be perceived as the most vulnerable targets. Consequently, they've been quick to adopt European electronic commerce laws as their template," notes Catherine McGrail, CEO of Miami-based Clavex, a digital identity authentication solutions provider focused on the Latin American banking sector.

Brazil already has in place a well-established PKI. Brazil's government took aim at secure authentication and management of online information in 2001, establishing standards and enabling legislation for

electronic certification and authentication, including a PKI framework called ICP-Brasil. The PKI system uses high-level digital certificates covering key information security risks, such as the confidentiality and integrity of data, verification of individuals and organisations sending data, and the legal non-repudiation of this information. Certificate Authorities under ICP-Brasil have the authority to register and oversee certificates. Ms MGrail anticipates that the number of corporate digital certificates issued in Brazil will grow from 200,000 currently to more than five million by the end of 2008.

Following Brazil's example in the region, "other countries that hadn't put these laws in place are now in the process of doing that," Ms McGrail says. "In Chile, for example, eight of the country's largest local banks recently got together to establish Certinet, a Certificate Authority that will issue certificates on behalf of the banks to address 'know your customer' due diligence. Costa Rica also has expressed interest in creating a PKI, as has Panama, while many other countries have e-commerce and digital signature laws in place."

Digitising bank accounts globally

The Hewlett-Packard Company's sizeable global business requires access to financial institutions the world over, but opening and closing all those bank accounts, not to mention their routine maintenance, is bogged down in time-consuming manual processes.

Not only is this labour-intensive process inefficient, it can also create significant risks for companies. "We have about 1,700 bank accounts around the world," says Sarah Jones, the London-based treasury director of the technology company's Europe, Middle East and Africa operations. "The process for updating authorised signers on all these accounts as someone joins or leaves the organisation is burdensome." Ms Jones adds, "It is not uncommon for the bank to have people on record that we had requested to be removed two years ago."

To build a better system, HP is at work on a proof-of-concept project with Citigroup and IdenTrust to digitise bank account opening, closing and maintenance. The US-based Transaction Workflow Innovation Standards Team (TWIST), a not-for-profit industry group of corporate treasurers, fund managers, banks and other entities, is also involved. "Under the auspices of TWIST, we've formed a Bank Mandate Working Group involving 14 large multinational corporations and nine banks," says Ms Jones. "Our mission is to create message standards to facilitate document exchange utilising digital identities as the means of authenticating signatories."

Ms Jones also cites other potential uses of digital identities. "A company like ours has a large global footprint and works with many suppliers. In today's world, supplier information is typically sent in paper form and re-keyed into back-office applications. How do we ensure that those bank details are bona fide, and how do we prevent re-keying errors? It is far better to have corporations exchanging sensitive information in an electronic, secure way, with the use of digital identities."

She adds that the need to authenticate transactions also applies inside a corporation. "When a request for funding comes in from a subsidiary or another part of the organisation, how do we know this is a valid request and how do we know that the person requesting the funding is an approved person? Digital identities can also be used to authenticate internal transactions."

Ms Jones points out that currently corporations are not governed by the same anti-money laundering rules that apply to financial institutions. But, she says, "I can see a time when they might be, and hence there will be a requirement for companies like HP to carry out 'know your customer' checks and controls. A digital identity can facilitate those processes too."

The business of identity authentication

Compliance with the many global rules governing Internet security will prove fruitful for companies in the identity authentication business. The Radicati Group, a Palo Alto, CA-based technology research firm, estimates that the identity management market software market currently amounts to more than $1.2 billion in worldwide revenues, and will top $8.5 billion by 2008. "I wouldn't call the market a bonanza yet, but it is slowly moving in that direction," says Aviva Litan, vice president and distinguished analyst at the technology research firm Gartner. "The market is being driven more by regulations than security and data protection. Up until this year, the purchases by companies [of identity authentication tools] were a blip on the radar screen. That's no longer the case."

There are already many examples of identity authentication at work in business and government. For example, the US Department of Defence has mandated Homeland Security Presidential Directive-12 to authenticate employees for physical and logon access. Beginning October 27th 2006, the federal government began issuing "smart" ID cards to new federal employees; existing employees will begin receiving the smart cards on October 27th 2007. In the financial industry, institutions are converting to systems that are compliant with standards created in 1993 by Europay, Mastercard and Visa, the three main payment organisations at that time. Known as EMV, these standards allow secure interoperation between embedded-chip cards and card processing devices. EMV financial transactions are less vulnerable to fraud than traditional credit card payments, which use the data encoded in a magnetic stripe on the back of the card. This is due to the use of encryption algorithms to provide card authentication to the processing terminal and the transaction processing centre.

Of the many forms of identity authentication technology, two stand out—biometrics and digital certificates. Biometric chips will be part and parcel of passports in the EU and Australia. In the private sector, use of PKI certificates is expected to grow, says Maria Lewis Kussmaul, founding partner of Boston-based investment bank America's Growth Capital. "Enterprise PKI using digital certificates offers a powerful solution for authentication, encryption, digital signing, access control and non-repudiation," Ms Kussmaul says.

> "Enterprise PKI using digital certificates offers a powerful solution for authentication, encryption, digital signing, access control and nonrepudiation."
>
> Founding Partner, America's Growth Capital

In addition, a fast-growing application of smart cards is digital identity authentication. The smart card stores an encrypted digital certificate issued by a Certificate Authority (CA), which contains information about the card holder. Smart cards are a powerful way to foil increasing fraud at cash machines. With an estimated 1.5 million units available worldwide, ATMs have become a regular feature of modern life, but so too has the threat of ATM crime. Mugging and "shoulder surfing"—where thieves stand near an ATM to obtain a user's PIN by looking over his shoulder or from the side—at cash machines are giving way to more sophisticated methods. The most common fraud technique is the use of skimming devices, which criminals attach to ATMs to capture the account information and PIN data stored on cards that have

magnetic strips. This trick does not work with smart cards, however, because their encrypted digital certificate ensures that the user's private key cannot be stolen.

Mr Johnson of the American Bankers Association says the pressures on all enterprises to conduct more robust identity authentication will intensify in the future. "What will morph into the next generation of regulations governing Internet security, I cannot say, but this is a dynamic process, with new threats coming every day," he says. "We're still at the beginning."

Keeping secrets secret

Pentagon Technologies Inc. is a major supplier of air handling equipment and particle counting instruments to large semiconductor manufacturers like Intel. In this rarefied world of high technology, maintaining business secrets is paramount. To keep electronic transactions between Intel and Pentagon Technologies under wraps and secure, the companies rely on digital certificates.

"We don't want a security breach to occur on our side that might affect our relationship with a key customer," explains Ross Lindell, chief information officer at Hayward, CA-based Pentagon Technologies. In the pre-Internet era, if an employee lost a file, for example, the security implications were limited generally to other employees. But, Mr Lindell says, in the online environment vulnerability increased manifold. "We now rely on digital certificates that tell us when our server is contacted by Intel's server that it is, indeed, Intel's server—and vice versa. The two servers become the two players in the transaction."

When Pentagon Technologies receives a purchase order or pricing requests from Intel, the digital certificates ensure validity. Similarly, when Intel receives an electronic invoice from Pentagon Technologies, its server authenticates and verifies the origin of the document. "In addition to the accounts receivable issue, the certificate obviates our liability to Intel in the event we cause a loss on their side," Mr Lindell says. "They also can be assured there is a good trail of documentary evidence of our transactions from a compliance standpoint. We've kept track down to the serial number of each one of the components we've supplied them."

Conclusion

Regulatory momentum is nurturing the development of the identity authentication market. A surge in Internet crimes, including "man in the middle" attacks, money laundering and identity and data theft, has spurred governments worldwide to take action by issuing a wide range of regulations. Compliance with these new rules is directly or indirectly propelling global organisations to invest in a range of identity authentication tools. In addition, many companies fear Internet crime and are employing authentication technologies with or without regulatory pressure.

Many identity authentication technologies answer the need for basic compliance, and each has its own pros and cons. Multifactor authentication is the most secure method of verifying identities and the integrity of data. Of particular merit is the use of PKI-based digital certificates with hard tokens, an approach that will be promoted by the US government and others as the preferred method in many regions of the world. However, each country is creating its own domestic PKI and, therefore, there is a lack of interoperability.

Appendix I
Major Regulations Affecting Identity Management

United States

Authentication in the Internet Banking Environment Guidance (2005)

Issued by the Federal Financial Institutions Examinations Council (FFIEC)

- Financial institutions offering Internet-based products and services to their customers should use effective methods to authenticate the identity of their customers.
- Single-factor authentication is inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. Where necessary, multifactor authentication, layered security or other controls should be implemented.
- Financial institutions are required to identify and assess the risks that may threaten customer information; develop, implement and test a written plan containing policies and procedures to manage and control these risks; and adjust this plan on a continuing basis to account for changes in technology, the sensitivity of customer information, or internal or external threats to information security.
- Security measures that financial institutions are obligated to consider include: shared secrets (information known by the customer and the authenticating entity), tokens (USB device that plugs into a computer, smart card, password-generating token that produces a unique pass-code), biometrics (physical characteristics), scratch card (non-hardware based one-time password), out-of-band authentication (techniques that allow identity verification through a channel not being used to initiate the transaction), internet protocol address location and geo-location and mutual authentication (customer identity is verified and target website is authenticated to the customer). It is left up to institutions to determine which, if any, of the security measures were appropriate, based on their individual risk assessment.
- Customer verification techniques include: positive verification (information from a person matches information available from trusted third party sources), logical verification (information, such as telephone and address, provided is consistent), and negative verification (information provided is not associated with fraudulent activity).

Sarbanes-Oxley Act, Section 302 (2002)

- Companies are required to have internal procedures to ensure accurate financial disclosure. The signing officers must certify that they are "responsible for establishing and maintaining internal controls" and "have designed such internal controls to ensure that material information relating to the company and its consolidated subsidiaries is made known to such officers by others within those entities."

Patriot Act, Section 326 (2001)

- As part of a Customer Identification Program (CIP), financial institutions will be required to develop procedures to collect relevant identifying information including a customer's name, address, date of birth, and a taxpayer identification number. Foreign nationals without a US taxpayer identification number could provide a similar government-issued identification number, such as a passport number.
- A CIP is also required to include procedures to verify the identity of customers opening accounts. Most financial institutions will use traditional documentation such as a driver's license or passport. However, the final rule recognises that in some instances institutions cannot readily verify identity through more traditional means, and allows them the flexibility to utilise alternate methods to effectively verify the identity of customers.
- As part of a CIP, financial institutions must maintain records including customer information and methods taken to verify the customer's identity.
- Institutions must also implement procedures to check customers against lists of suspected terrorists and terrorist organisations when such lists are

identified by Treasury in consultation with the federal functional regulators.
• The final rule also contains a provision that permits a financial institution to rely on another regulated US financial institution to perform any part of the financial institution's CIP.

Electronic Signatures in Global and National Commerce Act (2000)

• The so-called E-SIGN Act gives records sent over the Internet with digital and electronic signatures the same legal validity as signed paper documents. Electronic documents may be entered into evidence during court proceedings, since they are considered as valid as traditional paper documents.

Gramm-Leach-Bliley Act (1999)

• The Financial Privacy Rule requires financial institutions to provide a privacy notice that explains what information is collected about the consumer as well as where that information is shared, how it is used and how it is protected.
• The Safeguards Rule requires financial institutions to develop an information security plan. The plan must include: 1) Designating at least one employee to manage safeguards; 2) constructing a thorough risk management on each department handling the nonpublic information; 3) developing, monitoring and testing a program to secure the information; and 4) changing the safeguards as needed with the changes in how information is collected, stored and used.
• Financial institutions must take all precautions necessary to protect customers against pretexting (when someone tries to gain access to personal nonpublic information without proper authority.)

European Union

Money Laundering Directive (Directive 2005/60/EC)

• Member States shall prohibit their credit and financial institutions from keeping anonymous accounts or anonymous passbooks.
• Customer due diligence measures have to be applied in the following cases: 1) when establishing a business relationship; 2) when carrying out occasional transactions amounting to EUR 15,000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked; 3) when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold; 4) when there are doubts about the veracity or adequacy of previously obtained customer identification data.
• Customer due diligence measures shall comprise: 1) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source; 2) identifying, where applicable, the beneficial owner and taking risk-based and adequate measures to verify his identity so that the institution or person covered by this Directive is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts and similar legal arrangements, taking risk-based and adequate measures to understand the ownership and control structure of the customer; 3) obtaining information on the purpose and intended nature of the business relationship; and 4) conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's or person's knowledge of the customer, the business and risk profile, including, where necessary, the source of funds and ensuring that the documents, data or information held are kept up-to-date.

Value Added Tax Invoicing Rules (Directive 2001/115/EC)

• The Directive sets a single, simplified set of rules on invoicing valid throughout the EU.
• EU member states are required to recognise the validity of electronic invoices and allow cross-border electronic invoicing and electronic storage.
• Advanced electronic signatures or electronic data interchange may be used to guarantee the authenticity of origin and integrity of the contents of an invoice.

Community Framework for Electronic Signatures (Directive 1999/93/EC)

Market access:
• Member States must not make the provision of

certification services subject to prior authorisation of any kind.
• They may introduce or maintain voluntary accreditation schemes aimed at enhancing levels of certification-service provision. All conditions related to such schemes must be objective, transparent, proportionate and non-discriminatory.
• Member States may not limit the number of accredited certification service providers for reasons which fall within the scope of the Directive.
• Member States may make the use of electronic signatures in the public sector subject to possible additional requirements.
• Member States may not restrict the provision of certification services originating in another Member State in the areas covered by the Directive.
Legal effects of electronic signatures:
• An "advanced electronic signature" is uniquely linked to the signatory, capable of identifying the signatory, created using means that the signatory can maintain under his sole control and linked to the data which it relates in such a manner that any subsequent change of the data is detectable.
• The main provision of the Directive states that an advanced electronic signature based on a qualified certificate satisfies the same legal requirements as a handwritten signature. It is also admissible as evidence in legal proceedings.

Liability

• Member States must ensure that a certification service provider which issues a qualified certificate is liable vis-à-vis any person who reasonably relies on the certificate for defined reasons in the Directive.
International aspects
• Member States must ensure mutual legal recognition of electronic signatures. The Commission may make proposals to ensure that international standards and agreements applicable to certification services are fully implemented. With the agreement of the Council, the Commission may negotiate market access rights for Community undertakings in third countries.
• Member States must ensure that certification service providers and national bodies responsible for accreditation or supervision comply with Directive 95/46/EC on the protection of personal data .

Data Protection Directive (Directive 95/46/EC)

• Personal data of all citizens will have equivalent protection in all member states. Data must be processed fairly and lawfully; be collected for explicit and legitimate purposes and used accordingly; and be accurate.
• The Directive applies to "any operation or set of operations which is performed upon personal data," called "processing" of data. Such operations include the collection of personal data, its storage, disclosure, etc.
• The Directive applies to data processed by automated means (e.g. a computer database of customers) and to data that are part of or intended to be part of non-automated "filing systems" in which they are accessible according to specific criteria. The directive applies to data transfers on the internet.

Asia

South Korea

• The Basic Act on Electronic Financial Transactions, to take force in January 2007, is a new data-protection law aimed at providing increased security for online financial transactions and upholding consumer interests against online financial frauds. The centrepiece of the new law is immunity provisions for consumers against financial damage caused by incidents involving "fabrication or alteration" of means of access to customer accounts and by incidents arising from "electronic transfer or processing" of contracts and transactions.
• The Financial Supervisory Service issued consumer guidelines for electronic financial transaction security in December 2005. The guidelines list requirements such as installing security patches provided by financial institutions, avoiding using easy-to-guess passwords, and using secured and verified access to financial websites.
• Privacy guidelines issued from the Ministry of Information and Communication (published in June 2002, January 2002 and March 2003) define privacy-protection obligations of information and telecoms service providers in collecting, using, storing, transferring and deleting personal information. The latest set of guidelines requires companies to set operational standards to safeguard personal data from accidental or deliberate security breaches. Other requirements include departmental co-operation to maintain personal

data security at all organisational levels; control and monitoring of employee access to personal data; use of encryption algorithms for personal-data transmissions; and timely maintenance of information-security safeguards.

• The Law on the Promotion of Utilisation of Information and Communication Networks and the Protection of Data provides the basis for many programs to protect digital privacy. The law, which took effect in July 2001, specifically requires providers of online information to obtain users' approval before collecting and using their private information. Customers must also be notified of the transfer of their information from one provider to another as a result of a merger or acquisition.

• The Electronic Signature Law of 1999, under the jurisdiction of the Ministry of Information and Communication, stipulates the legal effects and certification requirements of digital signatures. Public or private organisations meeting certain eligibility requirements can become official certification agencies to endorse "signed" electronic contracts.

Japan

• The Personal Data Protection Law, practical rules and regulations of which took effect in 2005, requires businesses and organisations handling a large volume of personal data to take the following actions: specify the purpose of using personal data; use personal data only for the stated purposes; follow appropriate procedures for collecting personal data; safeguard personal data against loss, system failure and leakage; disclose the purpose of using personal data; and comply with rightful requests for correction or deletion of personal data. They must not provide personal data to third parties without a rightful consent from the data subject.

• The Electronic Commerce Promotion Council of Japan (ECOM) issued its "Guidelines Concerning the Protection of Personal Data in Electronic Commerce in the Private Sector" in March 1998. The guidelines, which have yet to be updated, contain the following provisions but no specific penalties for violations: 1) Individuals using personal data in e-commerce should clearly specify, within the bounds of legitimate business, the purpose of collecting such data and the boundaries of necessary information for that purpose; 2) The use and disclosure of personal data collected legally should be limited to the stated purpose of collecting such data; 2) Reasonable security measures should be taken, both technically and organisationally, against such risks as unauthorised access to personal data or the loss, destruction, alteration and leakage of personal data; 3) Individuals engaged in collecting, using and disclosing personal data have the obligation to take sufficient care to maintain the confidentiality of personal data under the provisions of laws and regulations; and 4) Refusals by the subject of the personal data to the use or disclosure to third parties of previously collected personal data should be honoured with full faith.

Singapore

• The E-Commerce Consumer Protection Code of 1998 is intended to protect personal information of e-commerce consumers. The code was adopted by the CaseTrust, which is a joint project operated by the Consumers Association of Singapore, the Retail Promotion Centre and CommerceNet Singapore. CaseTrust is an accreditation scheme to promote good business practices among store-based and web-based retailers. Retailers that meet the criteria stipulated in the CaseTrust code of practice will be given a logo to display at their storefront or website.

• The Electronic Transactions Act (ETA) came into force in 1998. It provides a legal foundation for electronic transactions, and it gives predictability and certainty to the electronic formation of contracts. The ETA allows for electronic signatures and contracts to be used in courts of law.

Australia

• Under the Privacy Amendment (Private Sector) Act 2000, website operators that collect personal information online must take reasonable steps to ensure that Internet users know who is collecting their information and how it is used, stored and disclosed. The law also allows consumers to access their records and correct them if wrong. Organisations must protect people from unauthorised access and disclosure of personal information they hold.

• Also, website operators who handle personal information must address issues of data security, such as encryption. All websites must include a clearly identified privacy statement. An organisation in Australia may transfer personal information to someone in a foreign country only if it reasonably believes the recipient

of the information is subject to a rule of law that effectively upholds principles substantially similar to the National Privacy Principles, or if the individual consents to the transfer or, broadly speaking, the transfer is for the benefit of the individual.

• The Electronic Transactions Act 1999 identifies four types of requirements that can be met in electronic form: to give information, to provide a signature, to produce a document and to record or retain information. The law sets out matters such as the basic elements that an electronic signature method must satisfy.

India

• The Information Technology Act 2000 amended various laws to recognise digital signatures and evidence in software form. The Controller of Certifying Authorities (CCA) must first license certifying authorities (CAs), which then issue digital-signature certificates. The CCA also specifies the form and content of such certificates and sets ground rules for relationships between the CAs and subscribers. The act allows the recognition of foreign CAs, with prior approval of the government.

Latin America

Brazil

• Brazilian law (Medida provisória 2.200-2), passed in 2001, states that any digital document is valid for the law if it is certified by ICP-Brasil (the official Brazilian PKI) or if it is certified by other PKI and the concerned parties agree as to the validity of the document.

Mexico

• Reforms to the Consumer Protection Law issued in May 2000 address transactions made through electronic media, optic media or through any other new technology. It outlined the confidentiality and security of information that companies must provide to consumers, and it set requirements for how a supplier of a service must identify itself.

Chile

• Law 19,799 on electronic signatures and electronic documents provides protection against e-commerce fraud. The latter was also covered by Law 19,233, which deals mostly with other forms of cybercrime, including unauthorised access to computer systems, adulteration, robbery or destruction of data and programs, and deliberately spreading computer viruses.

• The legislature approved a law in January 2002 that validates digital documents and digital signatures, guaranteeing the secure identity of parties conducting online transactions and guaranteeing the confidentiality and integrity of encrypted documents and contracts that are exchanged online.

Colombia

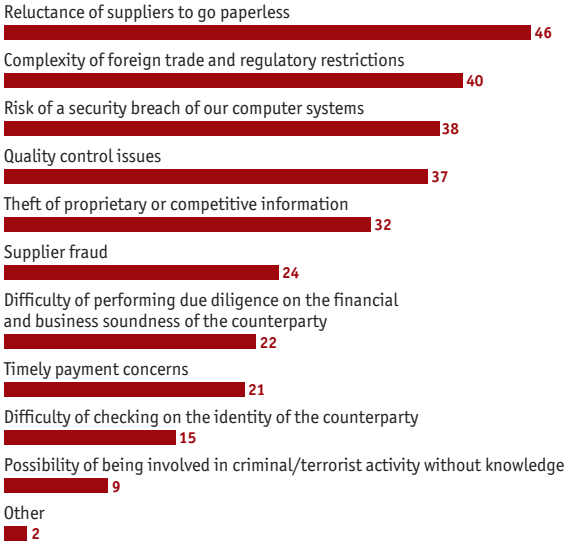
• The principal legislation approved in this area is Law 527 of August 1999. The law provides for the creation of an electronic or digital signature in the form of a coded number that is attached to an electronic message in such a way that it is invalidated if the message is altered. This number is to be agreed to by its owner and a certification agency or entity approved by the Superintendency of Industry and Commerce. Under the terms of the law, an electronic signature created in this way has the same legal effect as an ordinary written signature.

Appendix II: **Survey results**

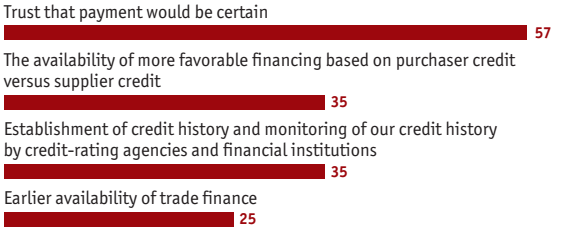
In May and June 2006, the Economist Intelligence Unit conducted an online survey of 127 executives from Europe, the Americas and the Asia-Pacific region. Our sincere thanks go to all who took part in the survey.

Please note that not all answers add up to 100%, because of rounding or because respondents were able to provide multiple answers to some questions.

1. What do you consider to be the greatest risks of automating your company's global supply chain?
Select 3 options (% respondents)

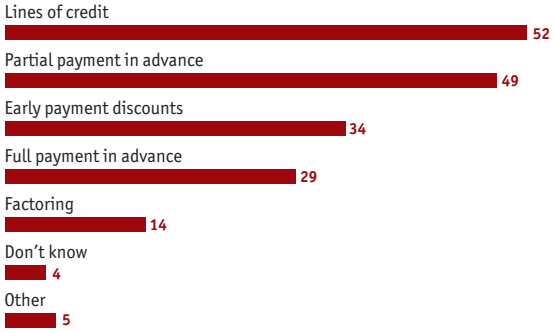


2. What would help your company to integrate its operations with the global supply chain?
Select all that apply (% respondents)



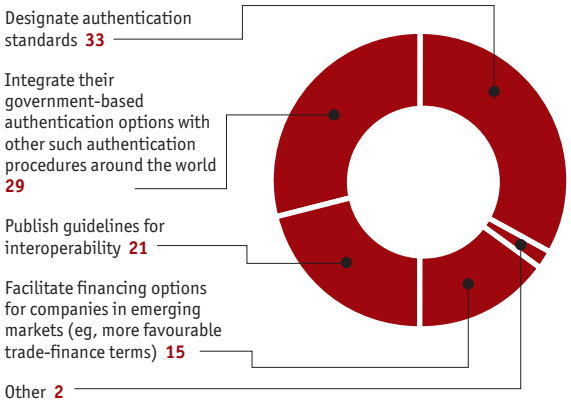
3. Does your organisation currently review supply chain vulnerability in the following areas or does it plan to do so in the next three years?
Select 3 options (% respondents)

4. Which of the following payment methods does your company use?
Select all that apply (% respondents)

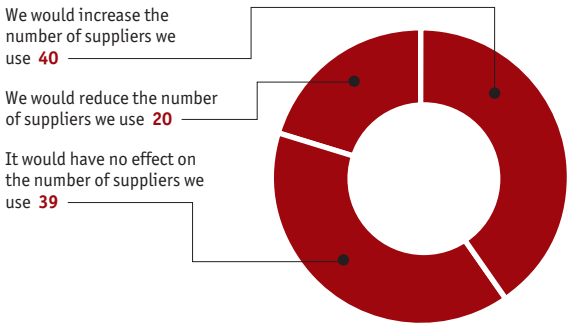


Source: Economist Intelligence Unit

5. What is the single most important step that individual governments and the UN could do to safeguard the global supply chain and ensure that more companies are integrated into it?
(% respondents)



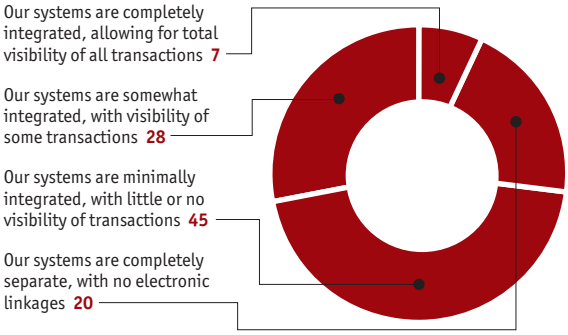
6. What effect would it have on your procurement practices, if your company were able to authenticate the financial stability of suppliers?
(% respondents)



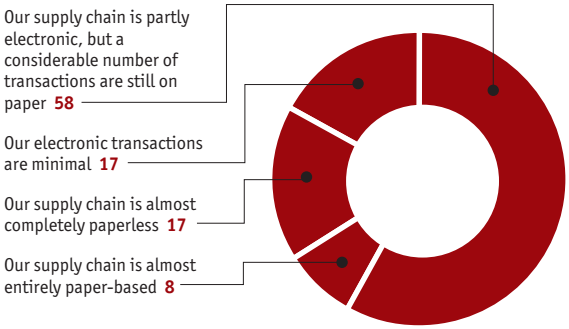
Source: Economist Intelligence Unit

7. What do you consider to be the greatest impediments to the implementation of a fully automated global supply chain for your company?
Select 3 options (% respondents)

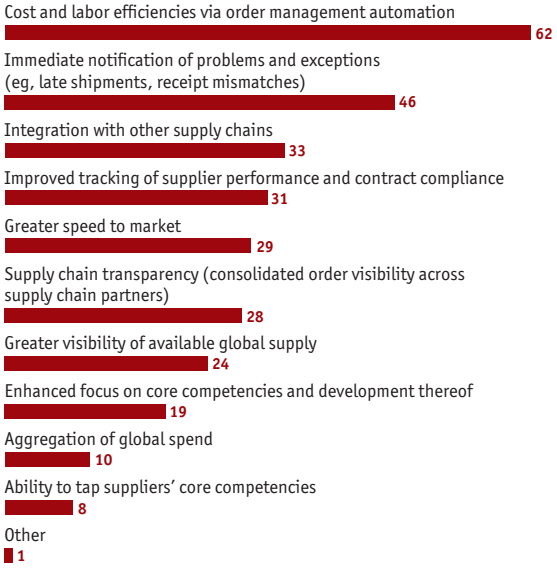
8. Which of the following statements best describes the level of integration between your organisation's procurement system and that of its suppliers?
(% respondents)



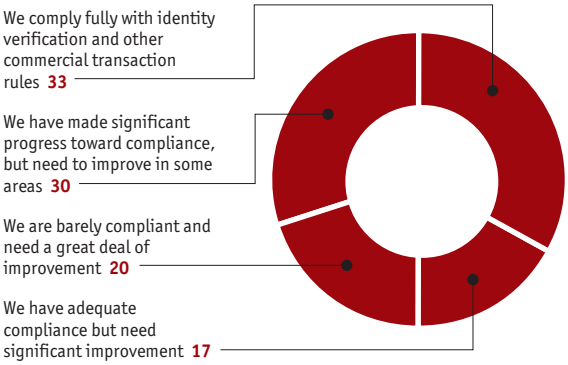
9. To what extent is your organisation's end-to-end supply chain paperless ie, managed electronically?
(% respondents)



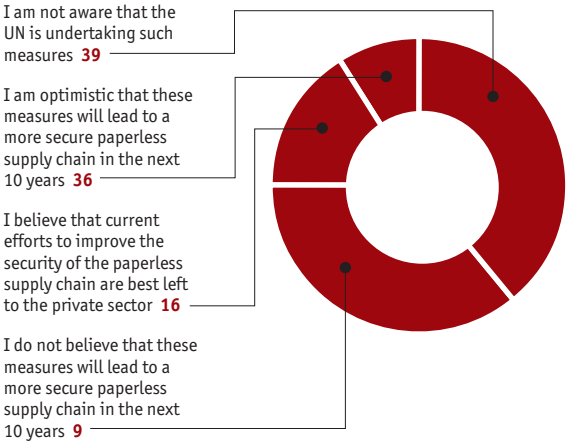
10. What do you consider to be the greatest advantages of automating your company's global supply chain?
Select 3 options (% respondents)



11. Which of the following statements best describes your organisation's level of compliance with regulations governing the global supply chain such as account authentication rules?
(% respondents)

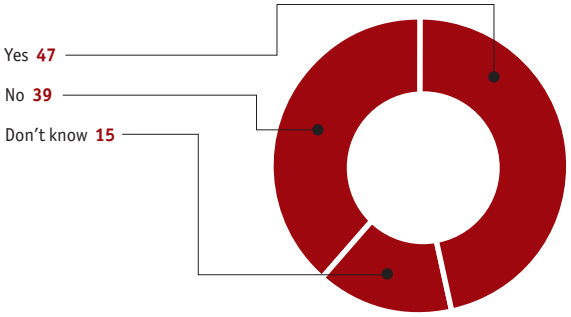


12. What is your opinion of efforts by the United Nations to standardise trade documents and to encourage governments to digitise the commercial forms completed by companies?
(% respondents)

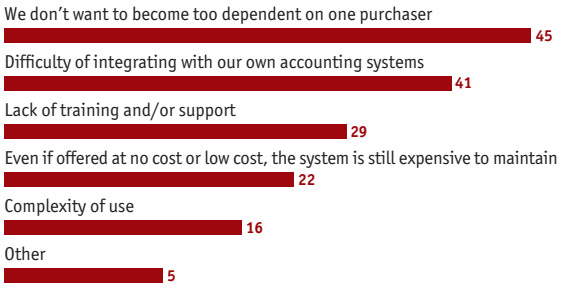


Source: Economist Intelligence Unit

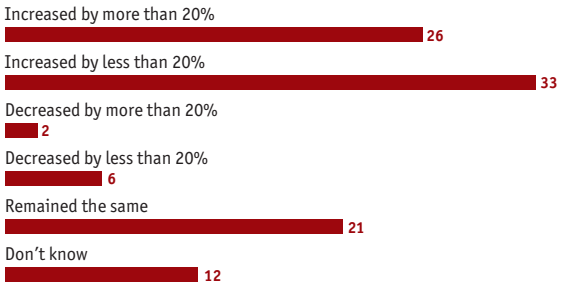
13. Does your company use any automated procurement systems offered by your purchasers?
(% respondents)



14. If not, why not?
Select all that apply (% respondents)

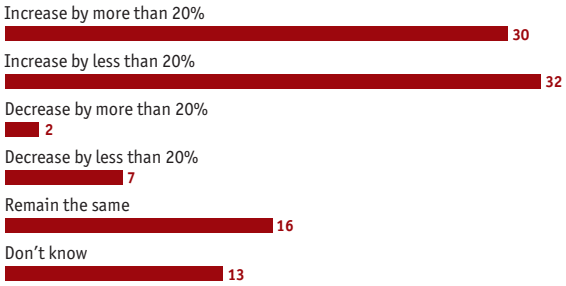


15. How has the number of your organisation's global suppliers changed in the past three years?
(% respondents)

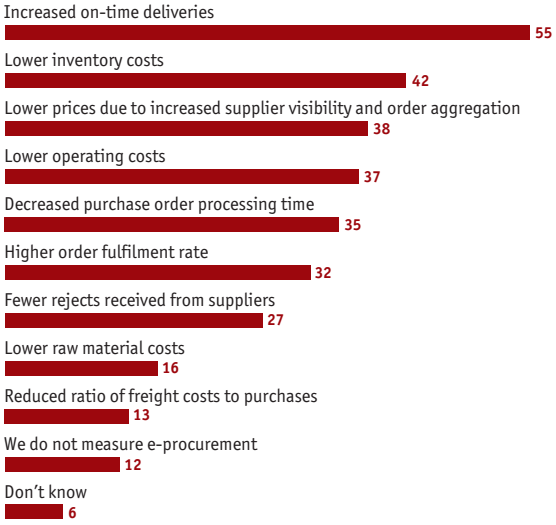


Source: Economist Intelligence Unit

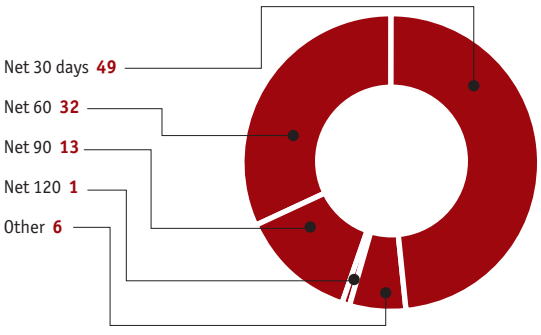
16. How is the number of your organisation's global suppliers likely to change in the next three years?
(% respondents)



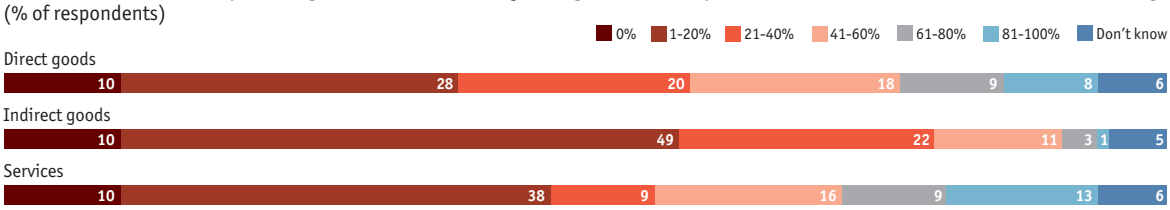
17. Which of the following measures does your organisation use to evaluate the success of its e-procurement efforts?
Select all that apply (% respondents)



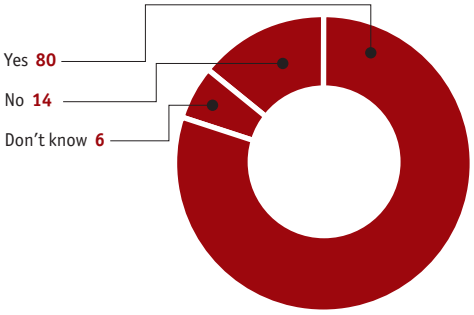
18. What are your company's payment terms?
(% respondents)



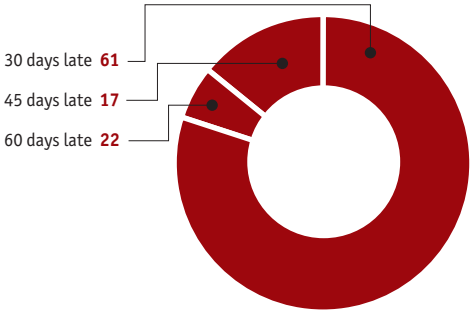
19. Please estimate what percentage of the total value of your organisation's e-procurement activities are focused on the following:
(% of respondents)



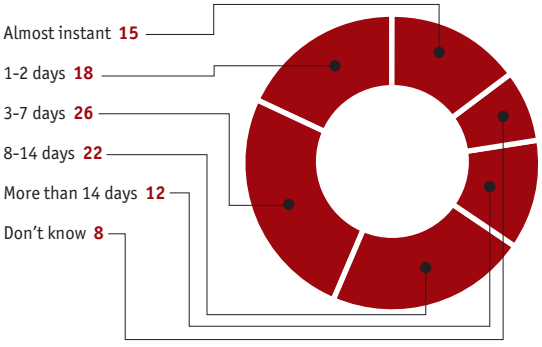
20. Does your company regularly pay on time?
(% respondents)



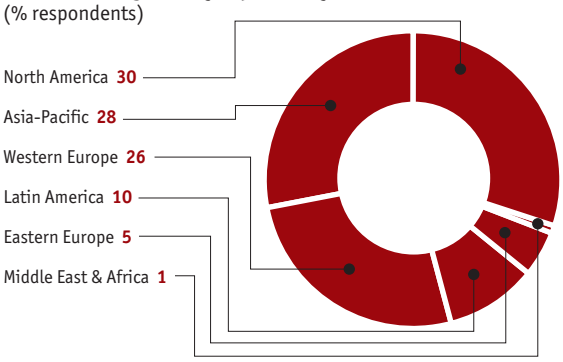
21. If not, what is your usual payment pattern?
(% respondents)



22. What is your company's average time for approval of payments to suppliers?
(% respondents)

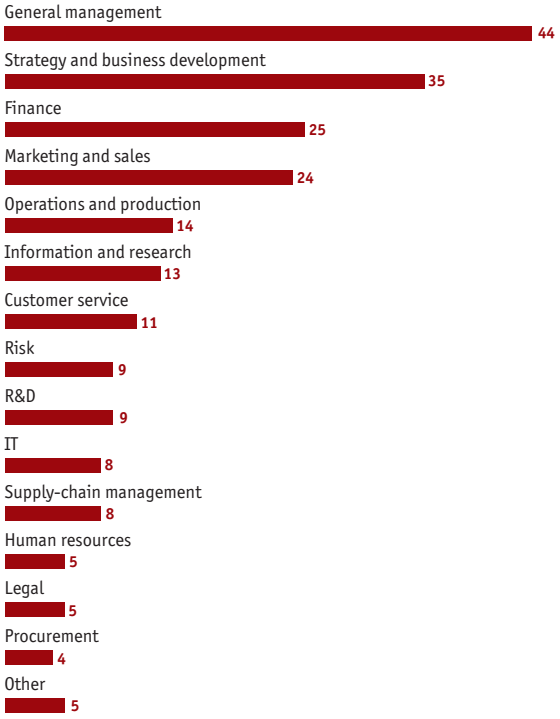


23. In which region are you personally based?
(% respondents)

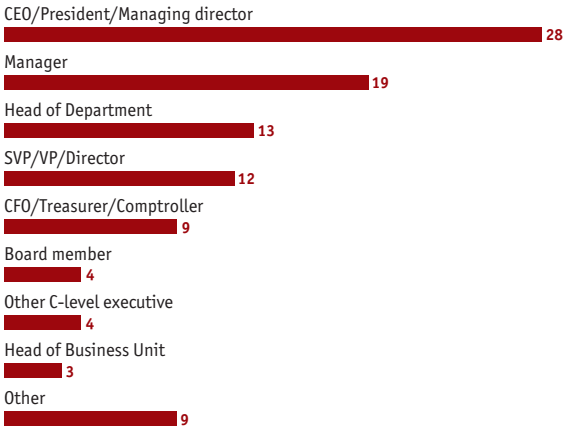


Source: Economist Intelligence Unit

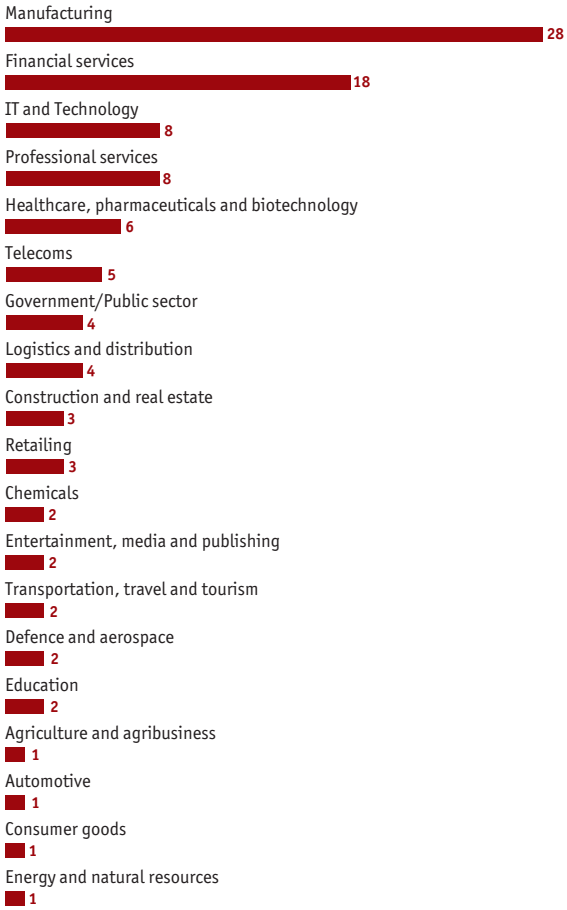
24. What are your main functional roles?
Please choose no more than three functions.
(% respondents)



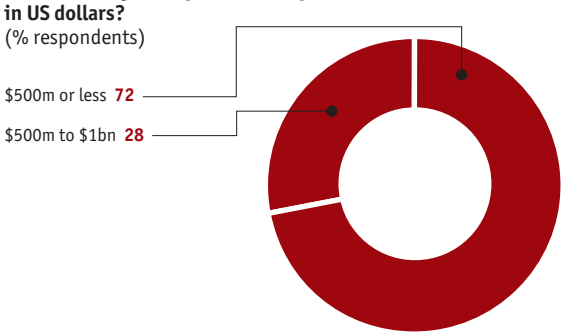
25. Which of the following best describes your title?
(% respondents)



26. What is your primary industry?
(% respondents)



27. What are your organisation's global annual revenues in US dollars?
(% respondents)



Source: Economist Intelligence Unit

Whilst every effort has been taken to verify the accuracy of this information, neither The Economist Intelligence Unit Ltd. nor the sponsor of this report can accept any responsibility or liability for reliance by any person on this white paper or any of the information, opinions or conclusions set out in the white paper.

LONDON
26 Red Lion Square
London
WC1R 4HQ
United Kingdom
Tel: (44.20) 7576 8000
Fax: (44.20) 7576 8476
E-mail: london@eiu.com

NEW YORK
111 West 57th Street
New York
NY 10019
United States
Tel: (1.212) 554 0600
Fax: (1.212) 586 1181/2
E-mail: newyork@eiu.com

HONG KONG
60/F, Central Plaza
18 Harbour Road
Wanchai
Hong Kong
Tel: (852) 2585 3888
Fax: (852) 2802 7638
E-mail: hongkong@eiu.com